令和元年度　情報セキュリティ研修

日本赤十字社における情報セキュリティについて

日本赤十字社
Japanese Red Cross Society

総務局　財政部
情報セキュリティ対策本部

目次

出典： 総務省『国民のための情報セキュリティサイト』を加工して作成
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/case/01.html

日本赤十字社
Japanese Red Cross Society

本研修の目的

情報セキュリティ研修を実施する主な目的は、組織の情報セキュリティに関する方針や行動指針を職員によく理解し、知ってもらうためです。

大半の職員がどれだけ情報の扱いに細心の注意を払っていても、それを守らない一部の職員がいる限り、組織の情報資産を守ることができません。サイバー攻撃や情報漏洩といったリスクから組織の情報資産を守るためには、職員一人ひとりが確実に情報セキュリティポリシーを守ることが必要なのです。そして、このような取り組みをきちんと行なうことで、組織価値や社会的信用の向上へとつながっていきます。

本研修では、コンピュータやインターネットについて基礎的な知識を身に付け、情報セキュリティに関する適切な考え方や対策を習得しましょう。

犯罪者からの攻撃を未然に防ぐため
職員のセキュリティ意識を向上させるため

情報セキュリティについて見識を高めることが大切です。

日本赤十字社
Japanese Red Cross Society

情報セキュリティとは

情報セキュリティという言葉は、一般的には、情報の機密性、完全性、可用性を確保することと定義されています。

情報セキュリティの3大要素

機密性	情報に関して、アクセスを認められた者だけがこれにアクセスできる状態を確保すること

機密性の保持とは
➡情報漏えい防止、アクセス権の設定、暗号の利用などの対策

完全性	情報が破壊、改ざん又は消去されていない状態を確保すること

完全性の維持とは
➡改ざん防止、検出などの対策

可用性	情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること

可用性の維持とは
➡電源対策、システムの二重化、バックアップ、災害復旧計画などの対策

日本赤十字社情報セキュリティ基本規程では「情報セキュリティ」を以下のように定義しています。

情報資産の機密性を保持し、正確性・完全性及び可用性を維持し、定められた範囲での利用可能な状態を確保すること

日本赤十字社
Japanese Red Cross Society

情報セキュリティ対策とは

コンピュータやインターネットに関連する技術は、急速に進歩し、変化し続けています。そのおかげで、私たちの生活は便利になり、仕事の効率も格段に上がっています。私たちが事業を運営する上で、コンピュータやインターネットは必要不可欠なものになっています。

しかし、コンピュータやインターネットを利用するのは善意の人たちばかりではありません。進歩したインターネット技術を悪用して、コンピュータウイルスや迷惑メールの送信、コンピュータへの不正侵入、インターネット上での詐欺行為、プライバシーの侵害などが発生しており、インターネットを利用する上で、私たちには様々な危険が降りかかっています。

私たちがコンピュータやインターネットを安心して使い続けられるように、大切な情報が外部に漏れたりウイルスに感染してデータが壊されたり、普段使っているサービスが急に使えなくなったりしないように必要な対策をすること。それが、**情報セキュリティ対策**です。

日本赤十字社
Japanese Red Cross Society

基礎知識１　インターネットでできること

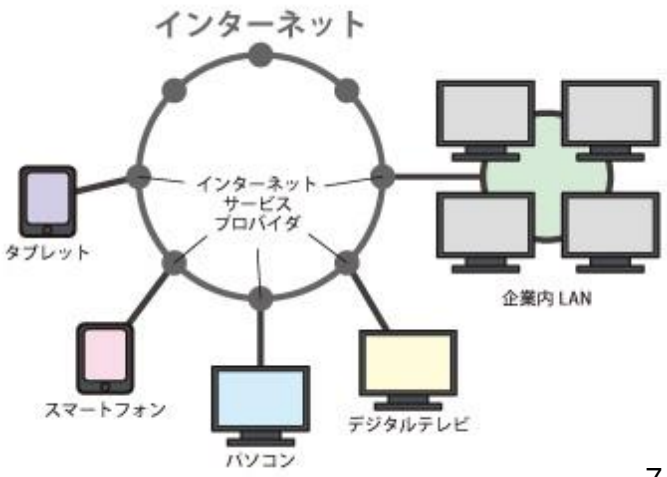
インターネットとは

　インターネットは、世界中のコンピュータなどの情報機器を接続するネットワークです。1990年ごろから、世界的に広く使われ始め、近年はその利活用が目覚しく進展してきました。現在では、私たちの生活や仕事などのさまざまな場面で使われる、不可欠な社会基盤（インフラ）となっています。

ネットワークとは

　複数のコンピュータを、ケーブルや無線などを使ってつなぎ、お互いに情報をやりとりできるようにした仕組みをネットワークと呼びます。

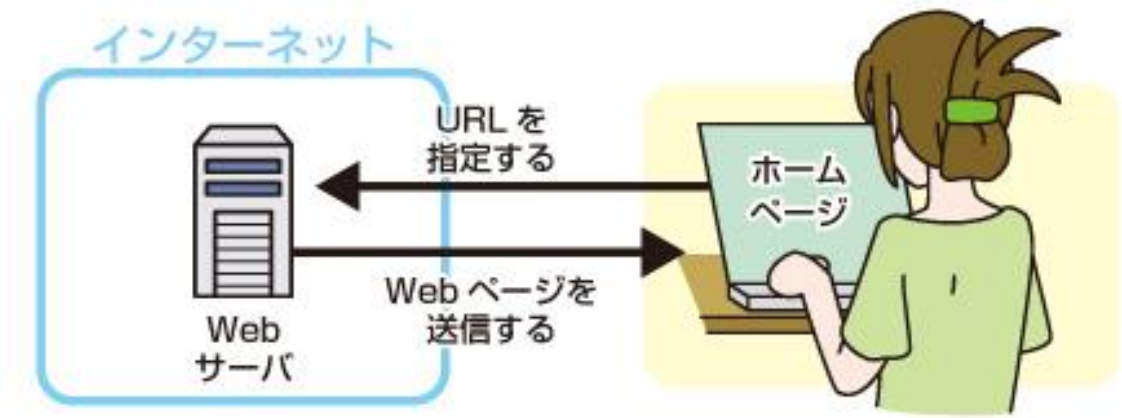
　インターネットは、家や会社、学校などの単位ごとに作られた１つ１つのネットワークが、さらに外のネットワークともつながるようにした仕組みです。外のネットワークと接続するために、ルータと呼ばれる機器や、インターネットサービスプロバイダと呼ばれる通信事業者のサービスを利用します。世界規模でコンピュータ同士を接続した、最も大きいネットワークといえます。



ホームページとは

インターネット上で情報を公開する仕組みを、ホームページと言います。ホームページのコンテンツ（内容）は、インターネット上に点在するWebサーバというホームページ公開専用のコンピュータのなかに保存されています。私たちの端末から、そのパソコンに命令を出し、情報を送ってもらうことで、ホームページを見ることができます。

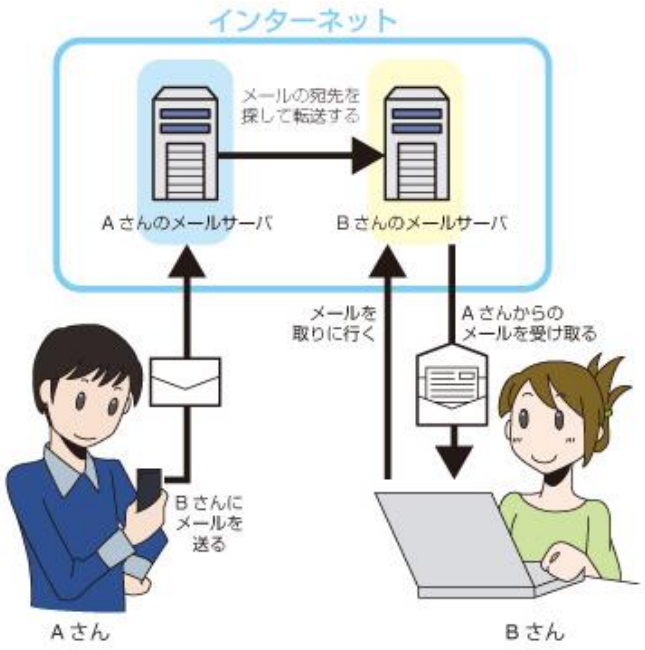
ホームページを閲覧する場合には、Webブラウザという専用のソフトウェアでURLを指定します。URLを指定すると、Webブラウザがインターネット上のWebサーバを探して、目的のホームページをコンピュータの画面上に表示します。



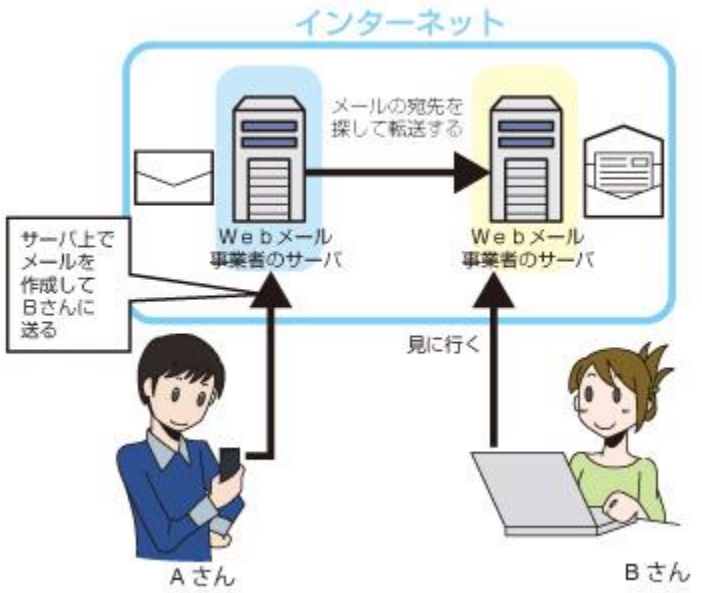
電子メールとは

電子メール(e-mail)とは、パソコンや携帯電話、スマートフォンなどの情報機器同士が、専用のメールソフトを使って、インターネットなどのネットワークを利用して情報をやりとりする機能です。やりとりできる情報は文章（テキスト）だけでなく、文書ファイルや画像などを添付ファイルとして扱うことができます。

電子メールの受取人はメールサーバにある自分のメールボックスに自分宛の電子メールを取りに行きます。



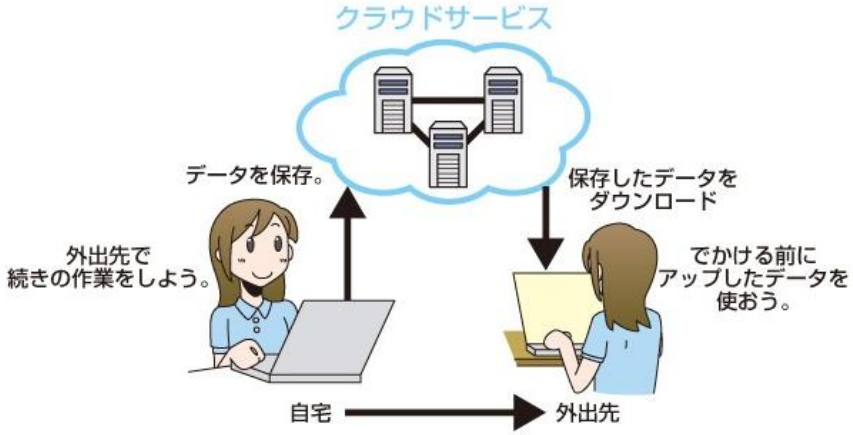
Web上でWebブラウザを使って送受信を行うWebメールは送受信された電子メールがサーバに蓄積されます。



クラウドサービスとは

クラウドサービスは、従来は利用者が手元のコンピュータで利用していたデータやソフトウェアを、ネットワーク経由で、サービスとして利用者に提供するものです。利用者側が最低限の環境（パーソナルコンピュータや携帯情報端末などのクライアント、その上で動くWebブラウザ、インターネット接続環境など）を用意することで、どの端末からでも、さまざまなサービスを利用することができます。

これまで利用者はコンピュータのハードウェア、ソフトウェア、データなどを、自身で保有・管理し利用していました。しかし、クラウドサービスを利用することで、機材の購入やシステムの構築、管理などにかかるとされていたさまざまな手間や時間の削減をはじめ、業務の効率化やコストダウンを図れる場合があります。



クラウドサービスは、主に以下の3つに分類されています。

◆ **SaaS（サース、サーズ：Software as a Service）**
インターネット経由での、電子メール、グループウェア、顧客管理、財務会計などのソフトウェア機能の提供を行うサービス。

◆ **PaaS（パース：Platform as a Service）**
インターネット経由での、仮想化されたアプリケーションサーバやデータベースなどアプリケーション実行用のプラットフォーム機能の提供を行うサービス。

◆ **IaaS（アイアース、イアース：Infrastructure as a Service）**
インターネット経由で、デスクトップ仮想化や共有ディスクなど、ハードウェアやインフラ機能の提供を行うサービス。HaaS（Hardware as a Service）と呼ばれることもあります。

日本赤十字社
Japanese Red Cross Society

基礎知識２　ＩＴ資産の脅威

どんな危険がある？

情報セキュリティに関する脅威はどんなものが考えられるでしょうか。

脅威とは、組織や企業に損害や影響を与える可能性であるリスクを引き起こす要因のことを言います。情報セキュリティにおける脅威は主に3つに分けられます。

物理的脅威	侵入、破壊、故障、停電、災害等
人為的脅威	誤操作、持ち出し、不正行為、パスワード管理不備等
技術的脅威	不正アクセス、盗聴、ウイルス、改ざん、消去、なりすまし等

かつて、サイバー攻撃をする人の目的は、自分の技術を見せつけるために相手のパソコンを正常に動作させないようにしたり、ホームページの内容を変更したりといった嫌がらせや迷惑行為などが大半でした。しかし、現在では金銭目的の犯行や詐欺行為、個人情報などの重要情報を盗み取ったり、国家レベルのテロ活動など、明確な悪意を持った犯罪が増加しています。

ターゲットも個人を狙ったものから企業・団体・政府組織を狙ったものまで幅広く、家庭用から企業・団体用まで、あらゆるネットワークが狙われるようになり、コンピュータやインターネットにおける危険性は多く存在しています。

インターネットを活用した脅威（犯罪や詐欺行為）

インターネットでは、様々な犯罪や詐欺行為などが増加しています。

- ◆偽物のホームページに誘導し個人情報などを窃取するフィッシング詐欺
- ◆電子メールなどで誘導してクリックしたことで架空請求などをするワンクリック詐欺
- ◆商品購入などで架空出品をしてお金をだましとるオークション詐欺
- ◆違法薬物など、法令で禁止されている物を販売する犯罪
- ◆公序良俗に反する出会い系サイトなどに関わる犯罪　　など多様な手口があります。

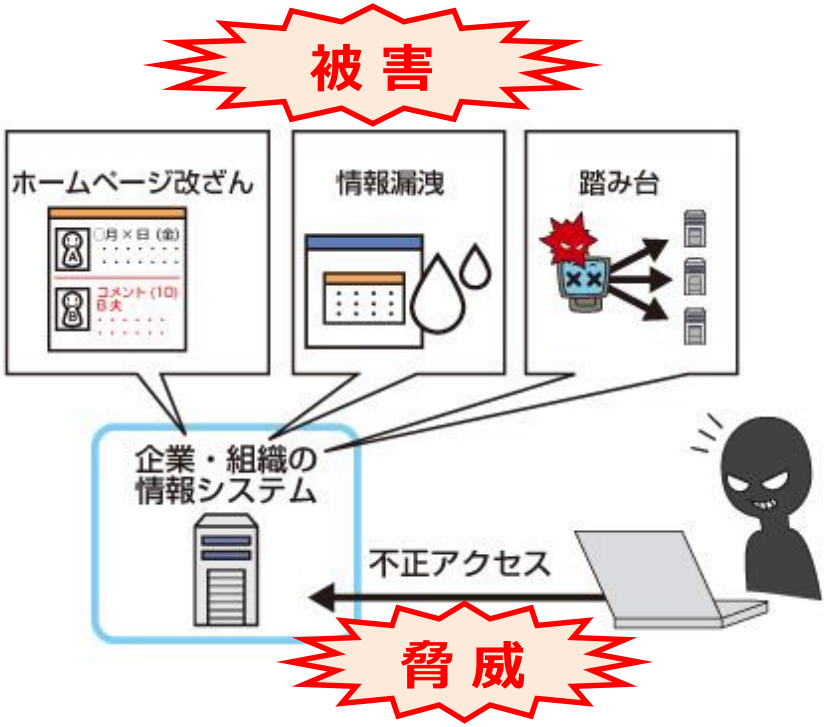
インターネットでの犯罪は金銭目的で行われることが多く、他人になりすます、ユーザIDやパスワード、プロフィールなどの個人情報を盗んで悪用するなど、さまざまな手法で行われます。

金銭目的以外では、相手への恨みや不満、興味本位などの動機から、攻撃や嫌がらせなどを目的として行われることもあります。

インターネットを活用した脅威（外部攻撃）

インターネットは世界中とつながっているため、インターネットにつながっている企業や組織のパソコンやシステムに不正で侵入される可能性は世界中のどこからでも考えられます。

不正アクセスとは、本来アクセス権限を持たない者が、サーバや情報システムの内部へ侵入を行う行為です。その結果、サーバや情報システムが停止してしまったり、重要情報が漏洩してしまったりと、企業や組織の業務やブランド・イメージなどに大きな影響を及ぼします。



被害者が加害者になりえる脅威

ウイルス感染したパソコンを踏み台にして外部から遠隔操作し、内部情報やシステムへの攻撃やインターネットを通じて外部へ攻撃をするコンピュータウイルスを「ボットウイルス」と呼びます。

攻撃者はボットウイルスに感染させたパソコンを踏み台にして攻撃をします。

- ◆感染したパソコンに含まれる情報を盗み出すスパイ活動
- ◆迷惑メールの配信
- ◆インターネット上のサーバへの攻撃
- ◆ボットを増やすための感染活動
- ◆犯罪者との取引　等

ボットに感染したパソコンの所有者は被害者ではありますが、そのパソコンから大量に迷惑メールを送信したり別のサイトを攻撃したりするため、その被害を受けた人から見るとボットウイルスに操られたパソコンの所有者が加害者として判断される場合があります。

補足　ホームページの改ざんによって、企業のホームページを閲覧した人たちを悪意のあるWebサイトへ誘導したり、ウイルスに感染させようとする手口もあるので注意！

意図的ではない脅威（ヒューマンエラー）

インターネットの脅威は、外部の攻撃者などにより意図的に行われるものばかりではありません。人による意図的ではない行為や、組織などの内部犯行、システムの障害などの事故も大きな情報セキュリティ上の脅威です。

人は意図的ではなく、操作ミスや設定ミス、紛失など、いわゆる「つい、うっかり」の過失（ヒューマンエラー）にも脅威はあります。電子メールの送り先を間違えたり、書類や記憶媒体の廃棄の方法を誤ったり、携帯電話やパソコンを紛失するといった過失が発生することで、顧客情報や機密情報が第三者へ漏洩することがあります。企業や組織における情報漏洩の原因の多くは、このような人の「つい、うっかり」やＩＴの使いこなし能力（ＩＴリテラシー）の不足によるものとされています。

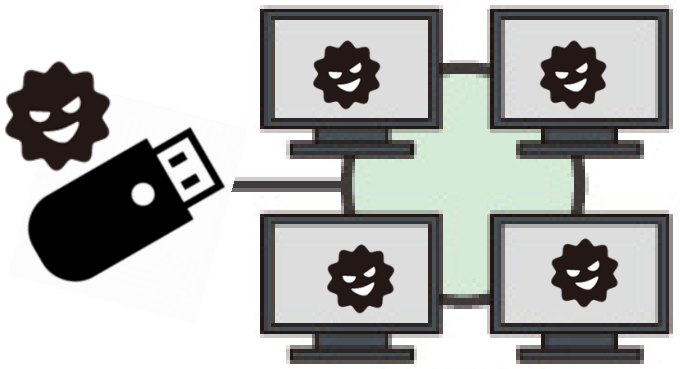
組織内部の脅威・閉域網ネットワーク内にある脅威

組織内の内部犯行も想定される脅威の一つです。例えば、悪意のある職員が企業の重要情報を競合企業へ提供したり、企業情報を買い取る業者へ販売したりすることが考えられます。アカウント管理やデータのアクセス権限を適切に設定し、アクセス記録を取ることで、人による脅威を未然に防ぐことができます。

また、ウイルス感染されたＵＳＢメモリを使用することで、社内の閉域網ネットワークにあるシステムがウイルス感染することも考えられます。

ウイルス感染する入口はインターネットだけではなく、インターネットが繋がっていないネットワークにあるパソコンにも、ウイルス感染する可能性があることを考慮し、セキュリティ対策を考える必要があります。

例：私物のＵＳＢメモリは使わない
　　ＵＳＢメモリを使う前にウイルスチェックをしてから使用する等



閉域網ネットワーク

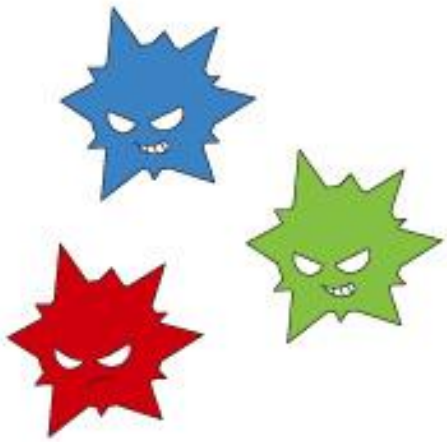
ウイルスとは

　ウイルスは、電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラムです。最近では、マルウェア（“Malicious Software”「悪意のあるソフトウェア」の略称）という呼び方もされています。

　数年前までは記憶媒体を介して感染するタイプのウイルスがほとんどでしたが、最近はインターネットの普及に伴い、電子メールをプレビューしただけで感染するものや、ホームページを閲覧しただけで感染するものが増えてきています。

　多くのウイルスは増殖するための仕組みを持っており、コンピュータ内のファイルに自動的に感染したり、ネットワークに接続している他のコンピュータのファイルに自動的に感染したりするなどの方法で自己増殖します。

　危険度が高いものの中には、ハードディスクに保管されているファイルを消去したり、コンピュータが起動できないようにしたり、パスワードなどのデータを外部に自動的に送信したりするタイプのウイルスもあります。



ウイルスの感染経路

◆ホームページの閲覧

現在のWebブラウザは、ホームページ上でさまざまな処理を実現できるように、各種のプログラムを実行できるようになっています。これらのプログラムの脆弱性を悪用するウイルスが埋め込まれたホームページを閲覧すると、それだけでコンピュータがウイルスに感染してしまう危険があります。

◆電子メールの添付ファイルやリンク

電子メールに添付されてきたファイルやリンクを開くと、それが悪意のあるプログラムであった場合はウイルスに感染してしまいます。最近は文書形式のファイルに見せかけて悪意のあるプログラムを実行させ、ウイルスに感染させる事例もあります。

◆信頼できないサイトで配布されたプログラムのインストール

あたかも無料のウイルス対策ソフトのように見せかけて、悪意のあるプログラムをインストールさせようとする「偽セキュリティソフト」の被害が増えています。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、利用者を偽のウイルス対策ソフトを配布するWebサイトに誘導する方法です。

◆ USBメモリからの感染

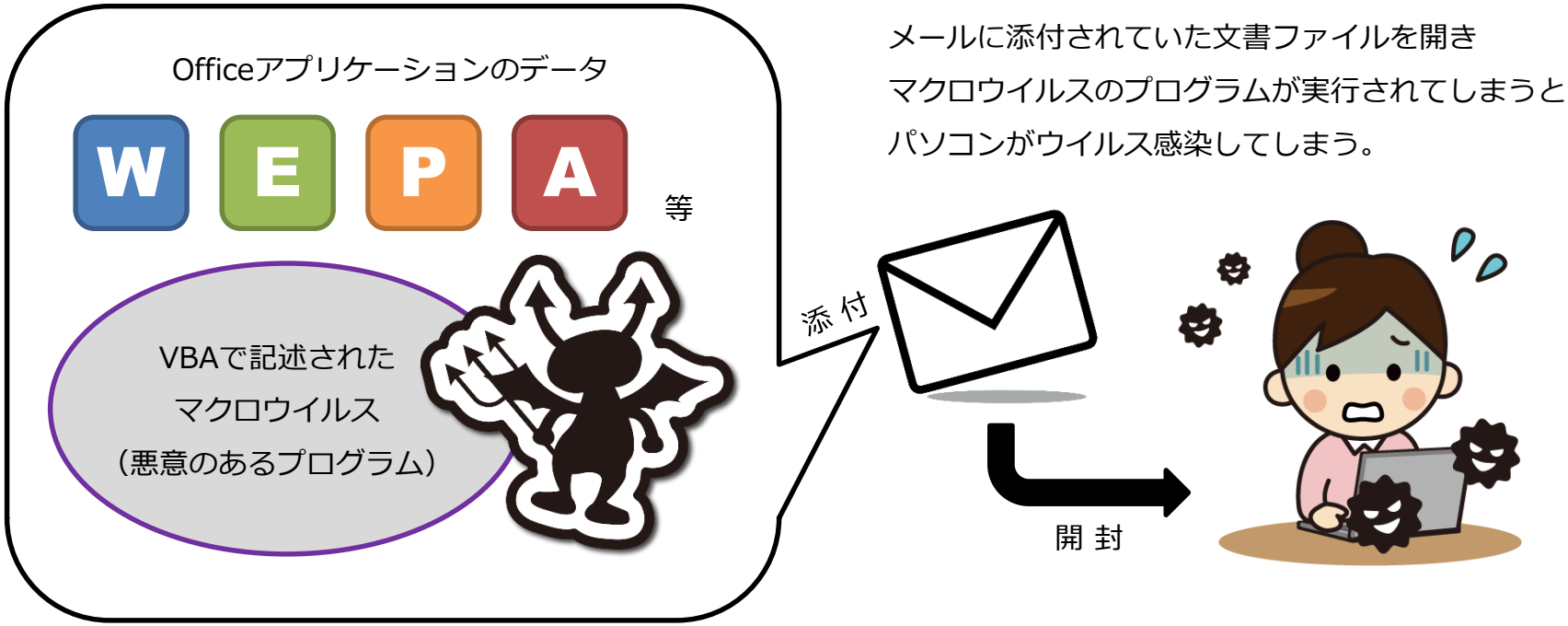
多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウイルスがあります。このようなウイルスの中には、感染したコンピュータに後から差し込まれた別のUSBメモリに感染するなどの方法で、被害を拡大させるものもあります。

ウイルスの感染経路

◆マクロプログラムの実行

マイクロソフト社のOfficeアプリケーション（Word、Excel、PowerPoint、Accessなど）には、特定の操作手順をプログラムとして登録できるマクロという機能があります。このマクロ機能を利用して感染するタイプのウイルスをマクロウイルスと呼びます。

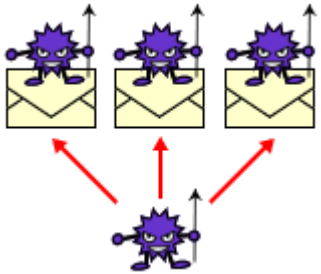
Officeアプリケーションでは、マクロを作成する際に、高度なプログラム開発言語であるVBA（Visual Basic for Applications）を使用できるため、ファイルの書き換えや削除など、コンピュータを自在に操ることが可能です。そのため、マクロウイルスに感染した文書ファイルを開いただけで、VBAで記述されたウイルスが実行されて、自己増殖などの活動が開始されることになります。



日本赤十字社 Japanese Red Cross Society

ウイルスの主な活動

◆自己増殖



ウイルスの中には、インターネットやLANを使用して、他の多くのコンピュータに感染することを目的としているものがあります。特にワーム型と呼ばれるウイルスは、自分自身の複製を電子メールの添付ファイルとして送信したり、ネットワークドライブに保存されているファイルに感染したりするなど、利用者の操作を介さずに自動的に増殖していきます。

◆情報漏洩（じょうほうろうえい）

ウイルスによる情報漏洩は、大きく分類すると、コンピュータに保存されている情報が外部の特定のサイトに送信されて起こる場合と、インターネット上に情報が広く公開されて起こる場合があります。ウイルスによって漏洩する情報は、ユーザIDやパスワード、コンピュータ内のファイル、メール、デスクトップの画像など、さまざまです。情報漏洩を引き起こすタイプのウイルスには、利用者がキーボードで入力した情報を記録するキーロガーや、コンピュータ内に記録されている情報を外部に送信するスパイウェアと呼ばれるものなどがあります。コンピュータがこのようなウイルスに感染していたとしても、コンピュータの画面上には何の変化も起こらないことが多いため、利用者はウイルスに感染していることに全く気が付きません。

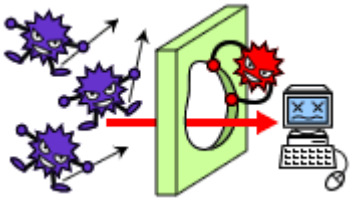
なお、漏洩した情報がインターネットに掲載され、公開されてしまった場合は、その情報をネットワーク上から完全に消去することは非常に困難です。

日本赤十字社 Japanese Red Cross Society

ウイルスの主な活動

◆バックドアの作成

感染したコンピュータの内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でも、コンピュータに外部から侵入しやすいように「バックドア」と呼ばれる裏口を作成するタイプのウイルスは極めて悪質なものです。この種のウイルスに感染すると、コンピュータを外部から自由に操作されてしまうこともあります。



◆コンピュータシステムの破壊

ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまでさまざまです。

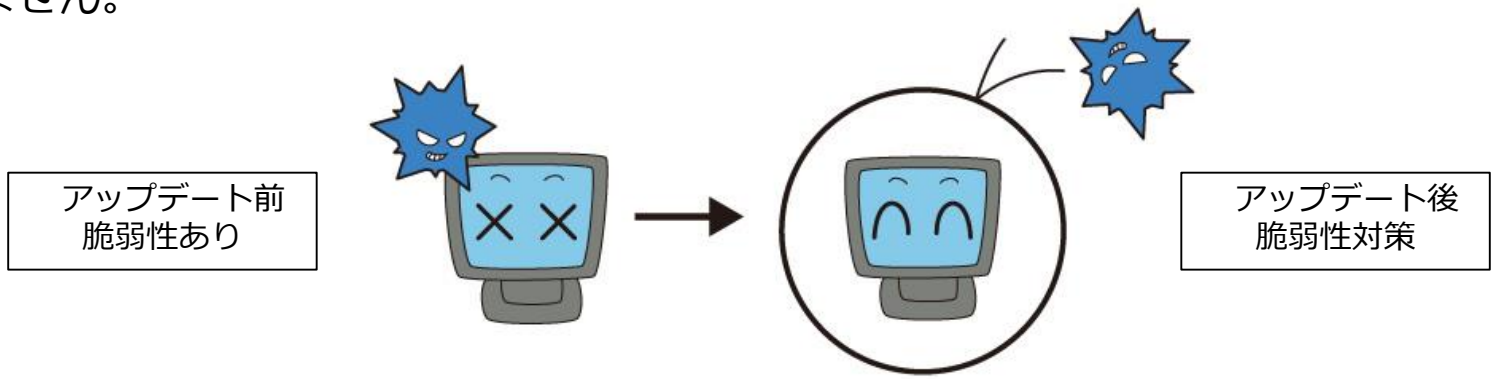
◆メッセージや画像の表示

いたずらを目的としたウイルスは、一定期間コンピュータ内に潜伏して、ある日時に特定のメッセージや画像を表示することがあります。ただし、最近はこのようないたずらを目的としたウイルスは減ってきています。近年では、パソコンやスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、復旧に金銭を支払うよう脅迫するランサムウェアと呼ばれるウイルスへの感染の被害が多くなっています。

脆弱性とは

脆弱性（ぜいじゃくせい）とは、コンピュータのOSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを言います。脆弱性が残された状態でコンピュータを利用していると、不正アクセスに利用されたり、ウイルスに感染したりする危険性があるため、情報セキュリティ上の大きな問題のひとつになっています。

脆弱性を塞ぐには、OSやソフトウェアのアップデートが必要となります。たとえば、Windowsの場合には、サービスパックやWindows Updateによって、それまでに発見された脆弱性を塞ぐことができます。ただし、また新たな脆弱性が発見される可能性があるため、常にOSやソフトウェアの更新情報を収集して、できる限り迅速にアップデートを行わなければなりません。



日本赤十字社
Japanese Red Cross Society

基礎知識３　ＩＴ資産の安全な運用

IDとパスワード

IDとパスワードは、パソコンなどの情報機器やWeb上のサービスを利用する際に、許可された者であるかを識別し、本人を確認するための重要な情報です。

他人に自分のユーザアカウントを不正に利用されないようにするには、適切なパスワードの設定と管理することが大切です。また、管理者は定期的なＩＤの棚卸を実施することが大切です。

安全なパスワードの設定（他人に推測されにくく、ツールなどで割り出しにくいもの）

(1) 名前などの個人情報からは推測できないこと
(2) 英単語などをそのまま使用していないこと
(3) アルファベットと数字が混在していること
(4) 適切な長さの文字列であること
(5) 類推しやすい並び方やその安易な組合せにしないこと
(6) パスワードを複数のサービスで使い回さない

悪い例
(1) 自分や家族の名前、ペットの名前
yamada、taro（名前）　19960628、h020315（生年月日）
(2) 辞書に載っているような一般的な英単語
password、baseball、soccer、monkey、dragon
(3) 同じ文字の繰り返しやわかりやすい並びの文字列
aaaa、0000（同じ文字の組み合わせ）
asdf、qwert（キーボードの配列）abcd、123456(安易な並び)

パスワードの保管方法

(1) パスワードは同僚などに教えないで、秘密にすること
(2) パスワードを電子メールでやりとりしないこと
(3) パスワードのメモをディスプレイなど他人の目に触れる場所に貼ったりしないこと
(4) やむを得ずパスワードをメモなどで記載した場合は、鍵のかかる机や金庫など安全な方法で保管すること

定期的なＩＤの棚卸し

(1) 退社した人や業務上必要のない職員に付与しているＩＤは削除すること。
(2) ＩＤに付与される権限の確認（見直し）をすること。

ウイルスに感染しないために

◆ ソフトウェアを更新する

ソフトウェアは常に最新のバージョンに更新することで、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥から侵入するウイルスを防ぐことができます。

◆ ウイルス対策ソフトを導入する

コンピュータにウイルス対策ソフトを導入する必要があります。ウイルス対策ソフトは、一般的にコンピュータの電源がオンであるときには常に起動した状態になり、外部から受け取ったり送ったりするデータを常時監視することで、インターネットやLAN、記憶媒体などからコンピュータがウイルスに感染することを防ぎます。

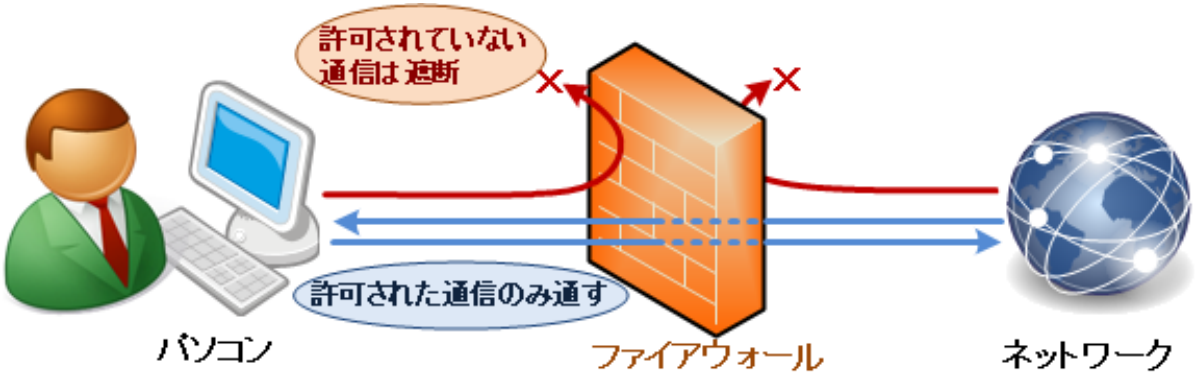
◆ 怪しいホームページやメールに注意する

ウイルスは悪性のホームページなどで配布されていたり、メールに添付されていたりなど、さまざまな経路でコンピュータに侵入してきます。悪性ホームページに接続する可能性のある迷惑メールや掲示板内などのリンクに注意する、不審なメールの添付ファイルを開かない、業務には関係ないホームページにはアクセスしないなどの対策が必要です。

不正アクセスに遭わないために

インターネットに接続したパソコンには、外部から自分の意図しない攻撃の通信が送られてくる場合があります。こうした不正アクセスをさせないためには、まず外部からの不要な通信を許可しないことが大切です。そのためには、通信の可否を設定できるファイアウォールを導入し、運用することが重要になります。

また、パソコンからインターネットに出る側の通信に制限をかけていない無制限の状態だった場合、犯罪者から見ても脇の甘い企業に見え、不審メールの送信等の「踏み台」にされる恐れがあります。

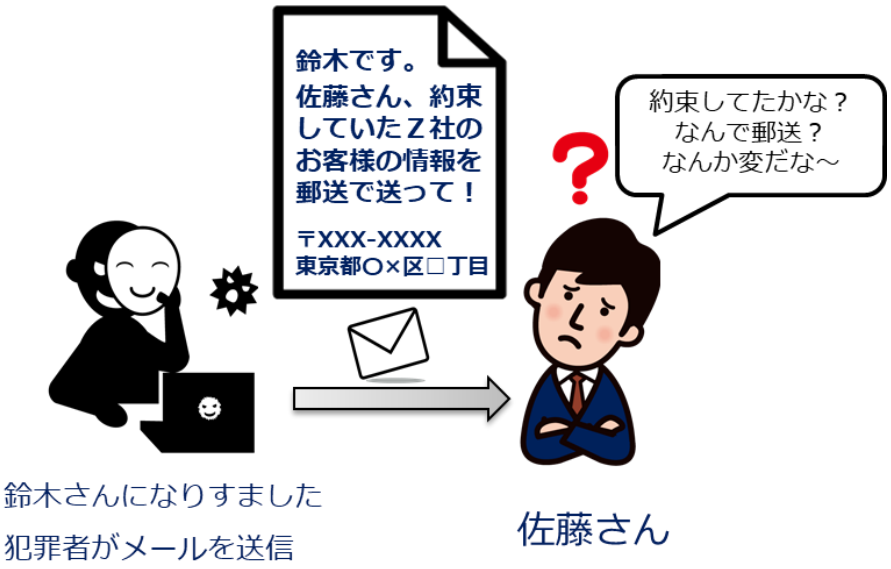


その他、不正アクセスをされる原因となる脆弱性への対策も必要になります。脆弱性が報告され、修正プログラムが配布されたら、速やかに適用するようにしましょう。

詐欺や犯罪に巻き込まれないために

インターネットを利用した詐欺や犯罪は、次々に新しい手口が登場しています。利用者の心構えとしては、普段からインターネットにおける詐欺や犯罪などの手口を知り、その対策について知識を深めておくことが大切です。

まず、インターネットやメール上のやりとりで、少しでも不審な点を感じたら、その情報の発信元や真偽を確認する姿勢が重要です。



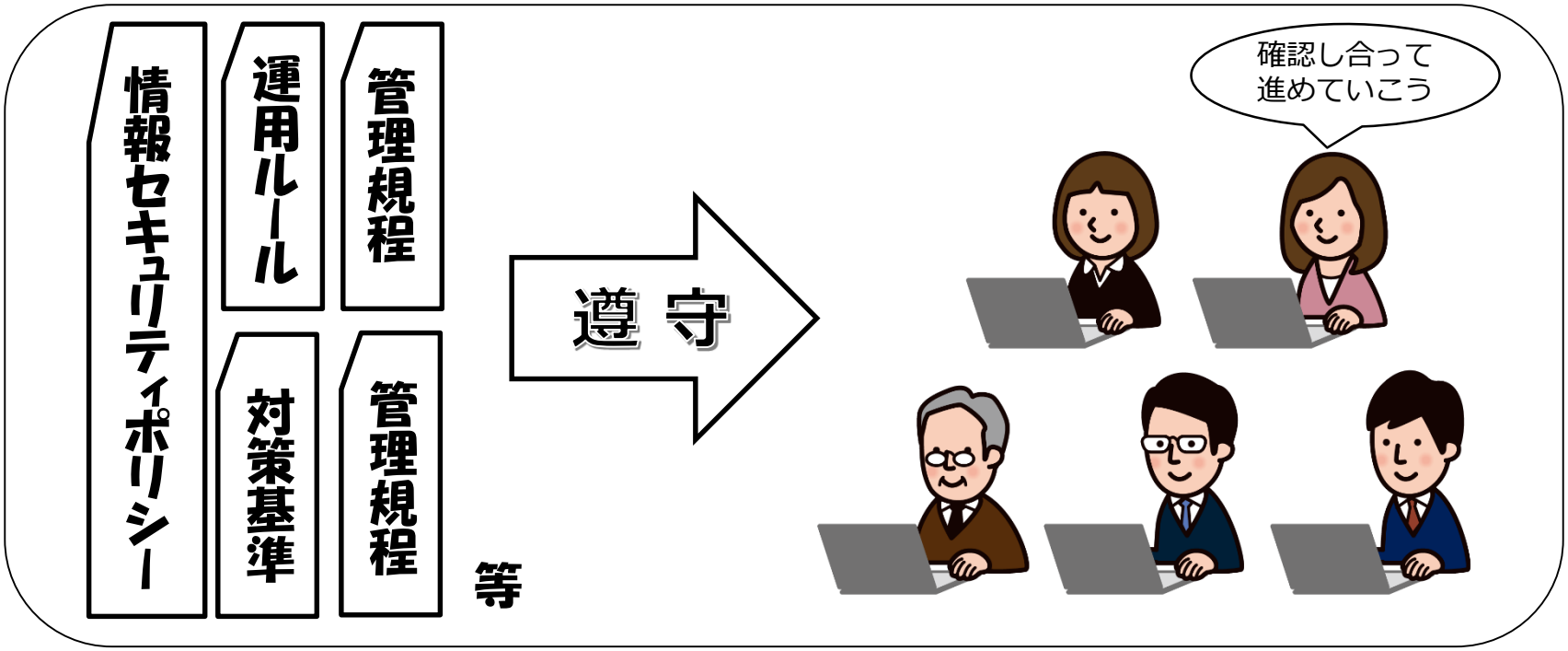
メールの内容を不審に思ったときは・・・

本人に確認して情報の真偽を確かめる

事故・障害への備え

事故や障害が完全に発生しないようにすることは困難です。しかし、その発生確率を下げたり、被害を最小限に抑えることは可能です。

過失による事故を未然に防ぐために、組織での情報セキュリティポリシーを遵守し利用や運用のルールを守ることはもちろん、人の過失に備えて、例えば二重の確認チェックなどを行うなど、こうした事故への対策をしましょう。



事故・障害への備え

コンピュータ障害や自然災害等によって情報やデータファイルが失われることを想定して日常的に重要情報のバックアップを取ることや、利用するシステムには盗難や紛失への備え、ファイル保護を行っているような信頼性の高い機能が備えておくことが必要です。

クラウドサービスのような外部業者のサービスを使っていた場合は、その業者側での障害で影響を受けることもあるため、事故や障害時の対応・対策を確認しておく必要があります。

コンピュータ障害

等

自然災害

等

日本赤十字社 Japanese Red Cross Society

各脅威における情報セキュリティ対策例

物理的脅威への主な対策例

物理的脅威	侵入、破壊、故障、停電、災害等

（１）サーバーの二重化

・必要に応じサーバ及び基幹サーバを二重化し、ミラーリング等により同一データを保持する。
・メインサーバに障害が発生した場合、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にする。

（２）予備電源の設置

・サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまでの間、十分な電力を供給する容量の予備電源を備え付ける。
・落雷等による過電流に対し、サーバ等の機器を保護するための措置を講じる。

（３）パソコン等の盗難防止

・盗難防止のため、ワイヤーの固定や保管庫への施錠等物理的措置を講じる。

（４）情報システム室等の入退室管理

・情報システム室等から外部に通じるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止する。

日本赤十字社 Japanese Red Cross Society

各脅威における情報セキュリティ対策例

人為的脅威への主な対策例

人為的脅威	誤操作、持ち出し、不正行為、パスワード管理不備等

（１）業務以外の目的での使用の禁止

・職員等は、業務以外の目的で情報資産の外部への持出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行わない。

（２）机上のパソコン等の管理

・職員等は、パソコン等及び電子記録媒体、情報が印刷された文書等について、第三者に使用及び閲覧されることがないよう離席時の端末のロックや電子記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じる。

（３）書類・紙媒体等の情報資産の取扱い

・業務上の情報が印字された書類・紙媒体、個人の特定が可能な写真、ネガ等が不要になった場合については、速やかにシュレッダー、溶解等の機密処理方法を用いて廃棄する。

（４）ID及びパスワードの管理

・自己の管理するIDを、他人に利用させない。
・パスワードは 、他人に知られないように管理する。
・パソコン等にパスワードを記憶させない。

日本赤十字社 Japanese Red Cross Society

各脅威における情報セキュリティ対策例

技術的脅威への主な対策例

技術的脅威	不正アクセス、盗聴、ウイルス、改ざん、消去、なりすまし等

（１）バックアップの実施

・ファイルサーバの冗長化対策に関わらず、必要に応じて定期的にデータのバックアップを実施する。

（２）アクセス記録の取得等

・各種アクセス記録及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存することとし、当該アクセス記録等が詐取、改ざん、誤消去等されないよう必要な措置を講じる。

（３）不正プログラム対策

・所掌するサーバ及びパソコン等に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させる。
・不正プログラム対策ソフトウェア及び同ソフトウェアの ウイルス定義ファイル（ パターンファイル ）を、常に最新の状態に保つ。

（４）アクセス制御

・ネットワーク又はシステムごとにアクセスする権限のない利用者がアクセスできないように、システム上制限する。

日本赤十字社
Japanese Red Cross Society

情報セキュリティ事故・被害の事例

情報セキュリティ事故・被害の事例

日本赤十字社 Japanese Red Cross Society

事例1　脆弱性を利用したランサムウェア

被害：2017年5月に150か国以上、35万台以上のコンピュータに感染。世界で40億ドルの被害額。
原因：Windowsの脆弱性（本事例はWindowsの脆弱性をついたものだが、別の要因で感染することもある）
補足：ランサムウェアとはウイルスの一種であり、感染すると端末内に保存しているデータが勝手に
暗号化されて使えない状態になったり、端末が正常に起動しなくなる。
また、感染した端末の中のファイルが暗号化されるだけではなく、その端末と接続された
別のストレージも暗号化される場合がある。
そして、その暗号化を解除するための身代金を要求する画面を表示させるというウイルス。

事例2　資料請求の情報が漏洩

被害：会社のホームページで、資料の請求のために登録された3万件以上の氏名、住所、年齢、
メールアドレスなどの個人情報が漏洩
原因：Webサーバの初歩的な設定ミス
補足：この他にも、基本的なサーバの設定ミスや脆弱性対策の不備が原因でホームページに登録された
個人情報が漏洩する事件は数多く発生
例）懸賞やプレゼントの応募者名簿、アンケートの情報、商品の購入者名簿など

事例3　ホームページの書き換え

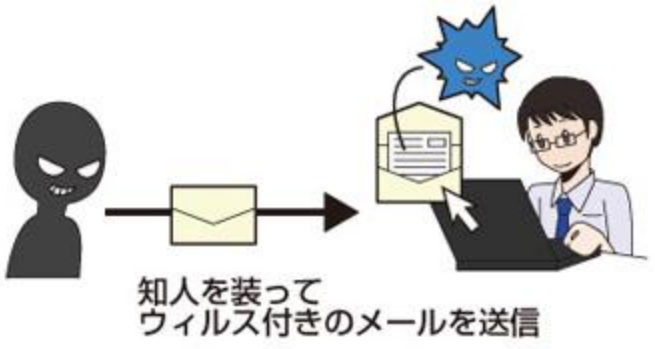
被害：自治体や大手企業、学校などのホームページが改ざん
原因：ある目的を持って特定の団体や企業を攻撃する場合と、
無差別に情報セキュリティ対策の甘いホームページを改ざんする場合に分類可能
補足：ホームページの改ざんは、FTPサーバの管理で安易なパスワードを設定していたり、既知の脆弱性を
そのまま残していたりと基本的な情報セキュリティ対策を怠ったことが原因であることが多い

事例4　中古パソコンによるデータの漏洩

被害：中古のパソコンを市販のデータ復元ソフトでハードディスクのデータを復元すると、
　　ある医療機関の診療報酬明細書の画像データが残されていた
原因：データが復元できないように処理して廃棄しなかった
補足：企業内の機密情報収集を目的として、中古パソコンを購入するという手口もあり、コンピュータや
　　ハードディスク、スマートフォン等は、必ずデータが復元できない状態にしてから廃棄すること

事例5　標的型攻撃で企業の重要情報が漏洩

被害：組織が所有している機密情報が、電子メールで外部に送信されていた
原因：ある職員の電子メールアドレスに、送信元を偽った標的型攻撃のメールが送られ、
　　職員は全く疑わずに業務用のパソコンで開封し、ウイルスに感染
補足：たった1通の標的型攻撃メールより、たった1台のパソコンがウイルス感染したことから、
　　重要な組織情報が盗まれるという事態に発生



日本赤十字社 Japanese Red Cross Society

情報セキュリティ10大脅威 2019

「情報セキュリティ10大脅威 2019」は、2018年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、情報処理推進機構（ＩＰＡ）が脅威候補を選出し、情報セキュリティ分野の研究者や企業の実務担当者等が審議し決定したものです。

「個人」向け脅威	順位	「組織」向け脅威
クレジットカード情報の不正利用	1	標的型攻撃による被害
フィッシングによる個人情報等の詐取	2	ビジネスメール詐欺による被害
不正アプリによる スマートフォン利用者への被害	3	ランサムウェアによる被害
メール等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した 攻撃の高まり
ネット上の誹謗・中傷・デマ	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	サービス妨害攻撃によるサービスの停止
インターネットバンキングの不正利用	7	インターネットサービスからの 個人情報の窃取
インターネットサービスへの不正ログイン	8	IoT 機器の脆弱性の顕在化
ランサムウェアによる被害	9	脆弱性対策情報の公開に伴う悪用増加
IoT 機器の不適切な管理	10	不注意による情報漏えい

出典：ＩＰＡ　情報セキュリティ10大脅威 2019　https://www.ipa.go.jp/security/vuln/10threats2019.html

日本赤十字社 Japanese Red Cross Society

情報セキュリティ10大脅威 2019

組織向け脅威

出典：ＩＰＡ　情報セキュリティ10大脅威 2019
https://www.ipa.go.jp/security/vuln/10threats2019.html

第1位　標的型攻撃による被害

企業や民間団体そして官公庁等、特定の組織から重要情報を窃取することを目的とした標的型攻撃が発生している。攻撃者はメールの添付ファイルや悪意のあるウェブサイトを利用し、組織のPCをウイルスに感染させる。その後、組織内部へ潜入し、組織内部の侵害範囲を拡大しながら重要情報や個人情報を窃取する。

補足：
攻撃の主な手口は、標的組織のパソコンをウイルスに感染させて機密情報を窃取する方法と標的組織が利用するクラウドサービスに不正アクセスし機密情報を窃取する方法がある。技術的な対策で100%防ぐことが難しく、職員のＩＴリテラシーの向上及びセキュリティ教育の実施等が必要とされる。

情報セキュリティ10大脅威 2019

組織向け脅威

出典：ＩＰＡ　情報セキュリティ10大脅威 2019
https://www.ipa.go.jp/security/vuln/10threats2019.html

第2位　ビジネスメール詐欺による被害

ビジネスメール詐欺（Business E-mail Compromise：BEC）は、取引先や経営者とやりとりするようなビジネスメールを装い、巧妙に細工されたメールのやりとりで企業の金銭を取り扱う担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。当初は主に海外の組織が被害に遭ってきたが、ここ数年で国内企業でも被害が確認されはじめ、2018年には日本語のビジネスメール詐欺の事例も確認された。

補足：
ビジネスメール詐欺の対策として、取引相手からいつもと異なる指示のメールを受けた場合は、電話やＦＡＸなどメール以外の方法で相手に事実確認を行ったうえで対応を行うようにする。

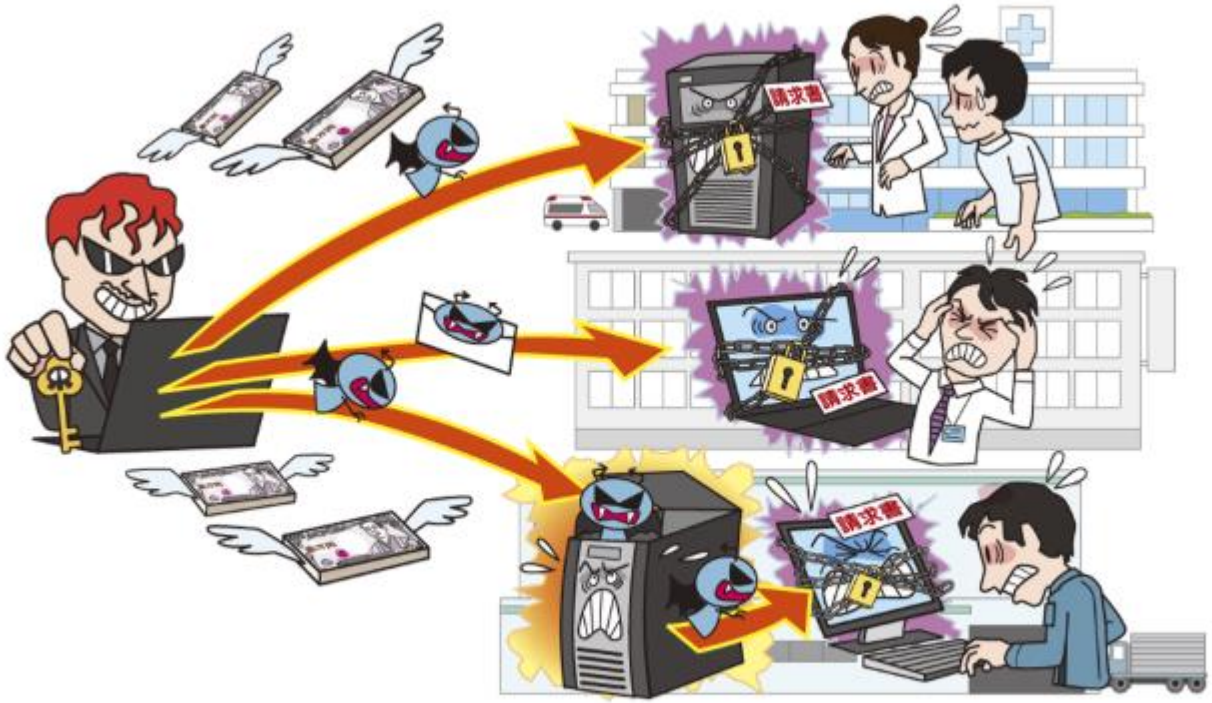
日本赤十字社 Japanese Red Cross Society

情報セキュリティ10大脅威 2019

組織向け脅威

出典：ＩＰＡ　情報セキュリティ10大脅威 2019
https://www.ipa.go.jp/security/vuln/10threats2019.html

第3位　ランサムウェアによる被害



PC（サーバー含む）やスマートフォンに保存されているファイルの暗号化や画面ロック等を行い、復旧に金銭を支払うよう脅迫するランサムウェアと呼ばれるウイルスへの感染が確認されている。組織においては、業務を遂行する上で必要な情報を暗号化された場合、事業継続にも支障がでるおそれがある。また、脅迫に従った場合、金銭的な被害も発生する。

補足：
ランサムウェアの被害は、ランサムウェアに感染したパソコンに限られず、感染したパソコンに繋がっているネットワーク上のサーバーにあるデータ等にまで被害が及ぶことがある。

日本赤十字社の情報セキュリティ

日本赤十字社の情報セキュリティ体系

日本赤十字社情報セキュリティポリシー

日本赤十字社 情報セキュリティ基本方針	日本赤十字社における情報セキュリティ対策に関する基本的な考え方を示したもの
日本赤十字社 情報セキュリティ基本規程	日本赤十字社における情報セキュリティ対策の目的、対象、管理体制及び管理者の義務等を規程したもの

日本赤十字社 情報セキュリティ対策基準	施設単位で整備される、情報セキュリティ対策として実施すべき具体的な手順（ルール）を定めたもの
日本赤十字社 情報セキュリティ緊急時対応計画	施設 にて情報セキュリティ事故が発生した場合における対応手順、及び警察機関・関係省庁を含んだ連絡体制、応急措置等を定めたもの

各部門システム 情報セキュリティ実施手順書	情報セキュリティ対策基準に基づき、各部門システムの詳細な情報セキュリティ対策の手順を定めたのも。

日本赤十字社の情報セキュリティ関連通知等

通知等	文書番号等	内容
「日本赤十字社情報セキュリティ基本方針」について	平成22年12月17日付 統情第20号社長通知	「情報資産のセキュリティ対策に万全を期す」日本赤十字社の情報セキュリティに対する基本姿勢、行動指針を示した
「日本赤十字社情報セキュリティ基本規程」の制定	平成22年12月17日付 本達丙第22号	日本赤十字社が遵守すべき情報セキュリティの基本事項を規定
個人情報を含む重要情報の適正管理について	平成27年6月9日 統情第31号	ー
支部・施設における情報セキュリティ対策基準の策定について	平成27年9月1日付 統情第44号	情報資産の性質や重要度に応じて講じなければならないセキュリティ対策の基準を定める（支部・施設単位で策定）
日本赤十字社情報セキュリティ緊急時対応計画の策定について	平成27年9月24日付 統情第53号	情報セキュリティインシデント発生時の本社・支部・施設の連絡体制や対応手順を定めたもの

日本赤十字社情報セキュリティ基本方針（一部抜粋）

目的

第１条 この規程は、日本赤十字社の保有する情報資産を保護・管理するために遵守すべき事項を定め、当該情報資産の機密を守り、故意や偶然という区分に関係なく、誤った使用や漏えい、改ざん、破壊等を防ぎ、情報を必要な時に確実に利用できるようにすることを目的とする。

適用範囲

第４条 この規程は、日本赤十字社の役員・職員、再雇用職員、嘱託職員、臨時職員、パートタイマー、日々雇い入れた者、その他日本赤十字社の情報資産を利用する者（以下「職員等」という。）に適用する。

職員等の責務

第５条 職員等は情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたり情報セキュリティポリシー並びに本社、支部及び施設で定める情報セキュリティ対策基準及び、実施手順を遵守しなければならない。

日本赤十字社情報セキュリティ緊急時対応計画（一部抜粋）

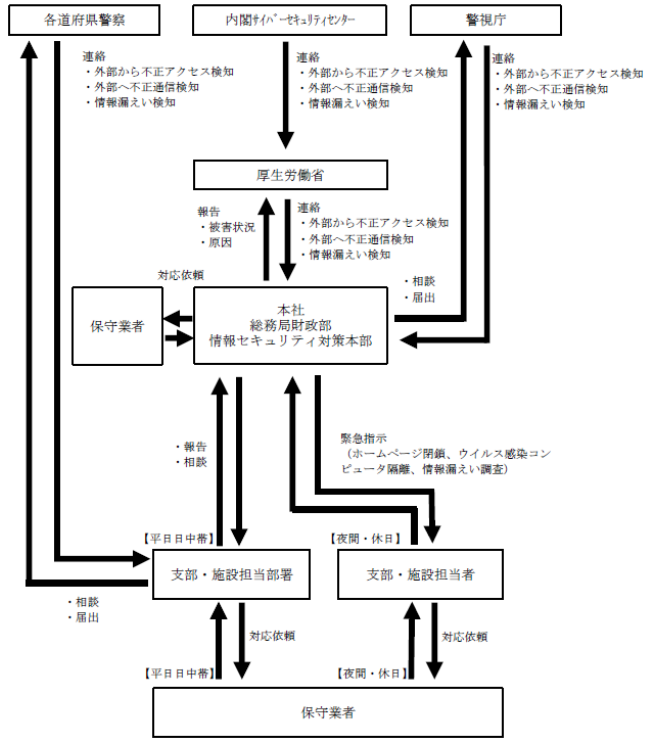
目的

本計画書は、日本赤十字社における 情報資産に対する事故、災害、情報セキュリティポリシー違反等による侵害が発生した場合、又は発生する恐れのある場合に備え、緊急時連絡体制、証拠保全、被害拡大の阻止、情報資産の復旧、再発防止等を計画し、その対応について定めることを目的とする。

緊急時連絡体制

緊急時の初動体制を円滑に行うため、 全社・本社・支部・施設・ 情報システム の単位で緊急時連絡体制を整備する。 また、報告事項は以下のとおりとし、別紙５「障害・事故等の発生及び再発防止等に関する報告書 」を総括情報セキュリティ管理者に提出する。

（１）対象となる情報資産
（２）障害区分
（３）概要（時間、場所、内容等）
（４）発生状況と被害の拡大予測
（５）発生原因
（６）その他留意事項



日本赤十字社緊急時全体体制図

情報セキュリティ対策本部の連絡先について

情報セキュリティ対策本部の連絡先

電話番号　　（03）3437-7593
メールアドレス　　infosec@jrc.or.jp